

CENTRALIZED CROSS-SYSTEM AUDITING OF DIGITAL IDENTITIES

HOW PRIMEID DISCOVER HELPED AN
AUTOMOTIVE SUPPLIER REGAIN AN OVERVIEW OF
ITS CERTIFICATE LIFECYCLES.

A multinational automotive supplier headquartered in DACH faces challenges by the sprawling usage of digital certificates within the organization.

CUSTOMER CHALLENGE

The automotive supplier operates several Certificate Authorities (CAs) internally using Microsoft Active Directory Certificate Services (AD CS). The use cases for the CAs range from protecting employee authentication credentials to issuing SSL certificates for securing servers, load balancers, and other elements in the corporate network.

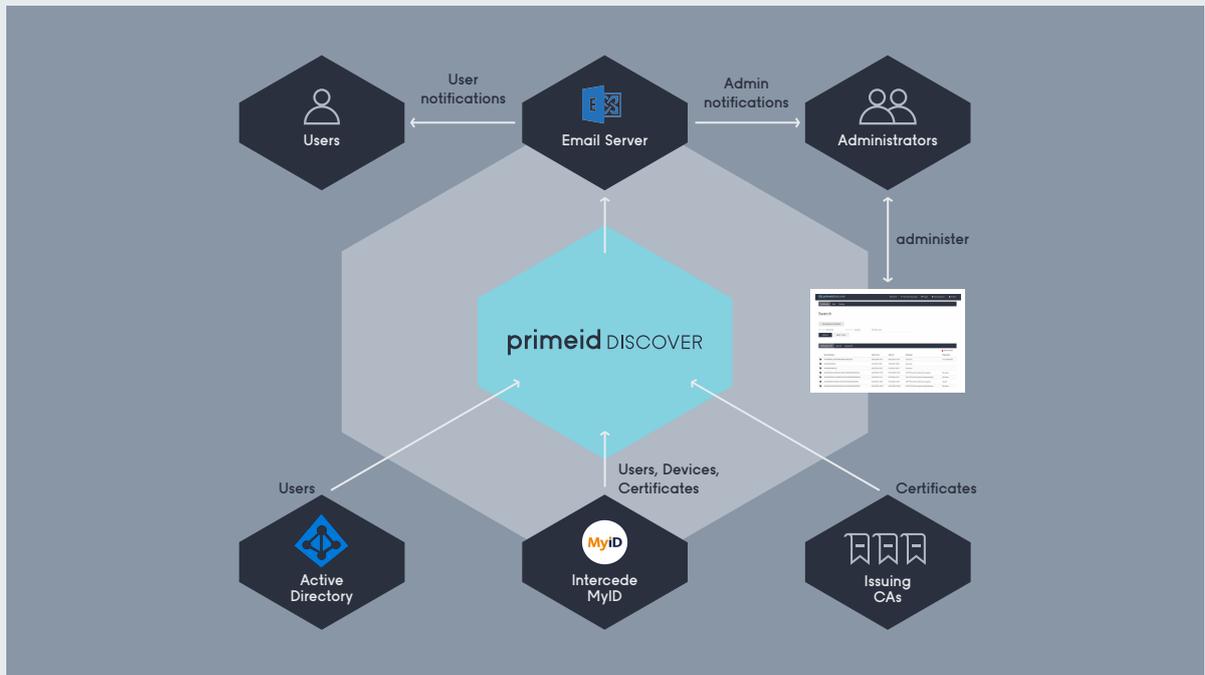
Keeping track of the life cycle of all the digital certificates issued is a major challenge for the global enterprise with over 100 sites and a large and constantly changing zoned network. Complicating matters further is that IT services are provided by many individuals spread across multiple sites, not all of whom have a strong security background and focus. Also, there is a typical churn rate. This combination puts the system at high risk for outages caused by certificates expiring at times and locations when it is least expected and tolerable for business continuity. For this reason, a central overview of all internally issued certificates is essential.

THE SOLUTION

CRYPTAS was able to provide a solution to gain and maintain an overview of all the automotive supplier's certificates: primeid DISCOVER.

primeid DISCOVER keeps track of all certificates issued by any of the company's CAs, the user identities, and authentication devices (smart cards) managed in the Intercede's MyID credential management system.

It also keeps track of the users in the corporate Active Directory. With this information, primeid DISCOVER reliably informs administrators and users via email messaging of any upcoming certificate expiry.



THE RESULTS

With primeid DISCOVER, the automotive supplier is now able to monitor the certificate status across its vast and heterogeneous IT infrastructure and thus prevent system outages due to unexpected certificate expiry. This saves the IT team a significant amount of time, and the company can avoid unexpected outages and costs.

The extended reporting capability gives the company a structured overview of the entire inventory of certificates, enabling efficient management of their lifecycles.